AMENDMENTS TO THE CLAIMS

Upon entry of this amendment, the following listing of claims will replace all prior versions and listings of claims in the pending application.

IN THE CLAIMS

Please amend claims 1, 4-13, 17, 19-28, 32, 35-43 and 47, cancel claims 2-3, 14-15, 18, 29-30, 33-34 and 45-46, and add new claims 48-58 as follows:

1. (Currently Amended) A computer-implemented method for adaptively filtering messages routed across a network by generating exception rules to rejection rules based on attributes of messages previously received and rejected, the method comprising:

receiving, by a security gateway, a first message from a user, the first message comprising a cookie session identifier field and a value of the cookie session identifier;

rejecting, by a message filter of the security gateway, the first message based on a rejection rule, the rejection rule rejecting messages having a cookie session identifier attribute, the cookie session identifier attribute indicating that the value of the cookie session identifier is different from a previously stored cookie session identifier value;

~~determining, for the first message by a learning engine of the security gateway, an attribute that triggered the rejection rule;~~

incrementing, by the learning engine ~~for the attribute~~, a count of the number of messages ~~rejected based on the attribute~~ from the user received via one or more user sessions within a predetermined amount of time and rejected based on the cookie session identifier attribute;

based on the count for the attribute, determining, by the learning engine, a frequency with which messages ~~having the attribute were rejected based on the rejection rule~~ with the cookie session identifier attribute were rejected based on the rejection rule;

generating, by the learning engine, an exception rule to the rejection rule ~~which rejected the messages with the attribute, responsive to the determined frequency exceeding a threshold~~ in response to determining that the frequency exceeds a threshold within the predetermined amount of time;

receiving, by the security gateway, a second message having the cookie session identifier attribute; and

allowing, by an adaptive filter of the security gateway, the second message, responsive to the exception rule.

2-3 (Cancelled).

4. (Currently Amended) The method of claim 1, wherein the rejection rule indicates that ~~attribute is one of a message component, a~~ value~~, a data type, and a length~~ of a cookie session identifier of a received message cannot be changed.

5. (Currently Amended) The method of claim 1, wherein the frequency is a weighted count of occurrences of the cookie session identifier attribute.

6. (Currently Amended) The method of claim 1, wherein the frequency is a direct count of occurrences of the cookie session identifier attribute.

7. (Currently Amended) The method of claim 1, further comprising comparing, by the message filter, that the value of the cookie session identifier and the previously stored cookie session identifier value ~~wherein the rejected messages are URL requests, each URL request having at least one URL component, the method further comprises: maintaining, by the learning engine, a frequency for each instance of a URL component, wherein the frequency is a function of a number of occurrences with which a URL component and its descendants were rejected by a rule; selecting, by the learning engine, a URL component according to a set of constraints; and generating, by the learning engine, an exception rule for the selected URL component and its descendants~~.

8. (Currently Amended) The method of claim ~~7~~1, wherein a user session represents communications between a client operated by the user and a server ~~the exception rule is generated by inferencing a scalar data type of the descendants of the selected URL component~~.

9. (Currently Amended) The method of claim ~~7~~1, further comprising storing, by the message filter, the value of the cookie session identifier~~wherein the set of constraints is selecting a URL component with a frequency exceeding a threshold and having no children with a frequency above the threshold~~.

10. (Currently Amended) The method of claim ~~7~~1, ~~wherein the set of constraints is selecting a URL component with the frequency exceeding a threshold~~ further comprising:

rejecting a third message based on a second rejection rule, the second rejection rule rejecting messages having a number of cookies different from a previously indicated number of cookies;

incrementing, by the learning engine, a second count of the number of messages from the user received via the one or more user sessions within the predetermined amount of time and rejected based on the cookie number attribute;

based on the second count, determining, by the learning engine, a second frequency with which messages with the cookie number attribute were rejected based on the second rejection rule;

generating, by the learning engine, an exception rule to the rejection rule in response to determining that the second frequency exceeds a threshold within the predetermined amount of time;

receiving, by the security gateway, a third message having the cookie number attribute; and

allowing, by the adaptive filter, the fourth message, responsive to the second exception rule.

11. (Currently Amended) The method of claim ~~7~~10, wherein the third message is a message responsive to an earlier message ~~the function is an aggregate of a number of occurrences with which the URL component was rejected by a rule and the number of occurrences with which descendants of the URL component were rejected by the rule~~.

12. (Currently Amended) The method of claim 10, wherein the third message~~s~~ is a message responsive to an earlier message, the earlier message providing the previously indicated number

of cookies ~~are URL requests, each URL request having at least one URL component, and the method further comprises: storing, by the security gateway, rejected URLs in a trie structure, wherein each node in the trie structure is associated with a URL component; maintaining, by the learning engine, a frequency for each node associated with a URL component, wherein the frequency is a function of a number of occurrences with which a URL component associated with a node and its descendants were rejected with a rule; selecting, by the learning engine, a node in the trie structure according to a set of constraints; and generating, by the learning engine, an exception rule for the selected node and its descendants~~.

13. (Currently Amended) The method of claim 1~~02~~, wherein the third message is a message sent from a client operated by the user to the server via the security gateway responsive to an earlier message sent from the server to the client ~~exception rule is generated by inferencing a scalar data type of the descendants of the selected node~~.

14-15 (Cancelled).

16. (Original) The method of claim 1, wherein the threshold is a product of a total number of messages over a time interval and a percentage of the messages that should be allowed to pass.

17. (Currently Amended) A system for adaptively filtering messages routed across a network by generating exception rules to rejection rules based on attributes of messages previously received and rejected, the system comprising:

a receiver which receives a first message from a user, the first message comprising a cookie session identifier field and a value of the cookie session identifier;

a filter which rejects the first message based on a rejection rule, the rejection rule rejecting messages having a cookie session identifier attribute, the cookie session identifier attribute indicating that the value of the cookie session identifier is different from a previously stored cookie session identifier value;

a learning engine, ~~for extracting, from the first message, an attribute of the message that triggered the rejection rule,~~ for incrementing, for the attribute, a count of the number of messages ~~rejected based on the attribute~~ from the user received via one or more user sessions within a

predetermined amount of time and rejected based on the cookie session identifier attribute, for determining, based on the count ~~for the attribute~~, a frequency ~~with which messages having the attribute were rejected based on the rejection rule~~ for which messages with the cookie session identifier attribute were rejected based on the rejection rule, and for generating an exception rule to the rejection rule ~~which rejected the messages with the attribute, responsive to the determined frequency exceeding a threshold~~ in response to determining that the frequency exceeds a threshold within the predetermined amount of time; and wherein

the filter applies the exception rule to subsequent messages to determine whether to allow the subsequent messages.

18. (Cancelled).

19. (Currently Amended) The system of claim 17, wherein the rejection rule indicates that ~~attribute is one of~~ a value of a cookie session identifier of a received message cannot be changed~~, data type, and length~~.

20. (Currently Amended) The system of claim 17, wherein the frequency is a weighted count of occurrences of the cookie session identifier attribute.

21. (Currently Amended) The system of claim 17, wherein the frequency is a direct count of occurrences of the cookie session identifier attribute.

22. (Currently Amended) The system of claim 17, wherein the message filter compares the value of the cookie session identifier and the previously stored cookie session identifier value ~~rejected messages are URL requests, each URL request having at least one URL component, and the learning engine further adapted to: maintain a frequency for each instance of a URL component, wherein the frequency is a function of a number of occurrences with which a URL component and its descendants were rejected with a rule; select a URL component according to a set of constraints; and generate an exception rule for the selected URL component and its descendants~~.

23. (Currently Amended) The system of claim 17, wherein a user session represents communications between a client operated by a user and a server ~~the set of constraints is selecting a URL component with the frequency exceeding a threshold and having no children with a frequency above the threshold~~.

24. (Currently Amended) The system of claim 17, wherein the message filter stores the value of the cookie session identifier ~~set of constraints is selecting a URL component with the frequency exceeding a threshold~~.

25. (Currently Amended) The system of claim 22, wherein ~~the function is an aggregate of a number of occurrences with which the URL component was rejected by a rule and a number of occurrences with which descendants of the URL component were rejected by the rule~~

the message filter rejects a third message based on a second rejection rule, the second rejection rule rejecting messages having a number of cookies different from a previously indicated number of cookies;

the learning engine increments a second count of the number of messages from the user received via the one or more user sessions within the predetermined amount of time and rejected based on the cookie number attribute, determining a second frequency with which messages with the cookie number attribute were rejected based on the second rejection rule based on the second count, and generating an exception rule to the rejection rule in response to determining that the second frequency exceeds a threshold within the predetermined amount of time;

the security gateway receiving a third message having the cookie number attribute; and

the adaptive filter allowing the fourth message, responsive to the second exception rule.

26. (Currently Amended) The system of claim ~~22~~25, wherein the third message is a message responsive to an earlier message ~~exception rule is generated by inferencing a scalar data type of the descendants of the selected URL component~~.

27. (Currently Amended) The system of claim ~~17~~25, wherein the third message~~s~~ is a message responsive to an earlier message, the earlier message providing the previously indicated number of cookies ~~are URL requests, each URL request having at least one URL component, and the~~

~~learning engine is further adapted to: store rejected URLs in a trie structure, wherein each node in the trie structure is associated with a URL component; maintain a frequency for each node associated with a URL component, wherein the frequency is a function of a number of occurrences with . which a URL component and its descendants were rejected with a rule; select a node according to a set of constraints; and generate an exception rule for the selected node and its descendants~~.

28. (Currently Amended) The system of claim ~~17~~25, wherein the third message is a message sent from a client operated by the user to the server via the security gateway responsive to an earlier message sent from the server to the client ~~set of constraints is selecting a node with the frequency exceeding a threshold~~.

29-30 (Cancelled).

31. (Original) The system of claim 17, wherein the threshold is a product of a total number of messages over a time interval and a percentage of the messages that should be allowed to pass.

32. (Currently Amended) A computer program product comprising: a computer-readable medium having computer program code embodied therein for adaptively filtering messages routed across a network by generating exception rules to rejection rules based on attributes of messages previously received and rejected, the computer program code adapted to:

receive a first message from a user, the first message comprising a cookie session identifier field and a value of the cookie session identifier;

reject the first message based on a rejection rule, the rejection rule rejecting messages having a cookie session identifier attribute, the cookie session identifier attribute indicating that the value of the cookie session identifier is different from a previously stored cookie session identifier value;

~~determine, for the first message, an attribute that triggered the rejection rule;~~

increment~~, for the attribute,~~ a count of the number of messages ~~rejected based on the attribute~~ from the user received via one or more user sessions within a predetermined amount of time and rejected based on the cookie session identifier attribute;

based on the count ~~for the attribute~~, determining a frequency with which messages ~~having the attribute were rejected based on the rejection rule~~ with the cookie session identifier attribute were rejected based on the rejection rule; and

generate an exception rule to the rejection rule ~~which rejected the message with the attribute, responsive to the determined frequency exceeding a threshold~~ in response to determining that the frequency exceeds a threshold within the predetermined amount of time;

receiving a second message having the cookie session identifier attribute; and

allowing the second message based on the exception rule.

33-34 (Cancelled).

35. (Currently Amended) The computer program product of claim 32, wherein the rejection rule indicates that ~~attribute is one of~~ a value of a cookie session identifier of a received message cannot be changed~~, data type, and length~~.

36. (Currently Amended) The computer program product of claim 32, wherein the frequency is a weighted count of the occurrences of the cookie session identifier attribute.

37. (Currently Amended) The computer program product of claim 32, wherein the frequency is a direct count of the occurrences of the cookie session identifier attribute.

38. (Currently Amended) The computer program product of claim 32, wherein the computer program code is further adapted to compare the value of the cookie session identifier and the previously stored cookie session identifier value ~~rejected messages are URL requests, each URL request having at least one URL component, wherein the computer program code is further adapted to: maintain a frequency for each instance of a URL component, wherein the frequency is a function of a number of occurrences with which a URL component and its descendants were rejected by a rule; select a URL component with the frequency exceeding a threshold and having no children with a frequency above the threshold; and generate an exception rule for the selected URL component and its descendants~~.

39. (Currently Amended) The computer program product of claim 32, wherein a user session represents communications between a client operated by a user and a server ~~the computer program code is further adapted to generate the exception rule by inferencing a scalar data type of the descendants of the selected URL component~~.

40. (Currently Amended) The computer program product of claim 38, wherein the computer program code is further adapted to store the value of the cookie session ~~function is an aggregate of a number of occurrences with which the URL component was rejected by a rule and the number of occurrences with which descendants of the URL component were rejected by the rule~~.

41. (Currently Amended) The computer program product of claim 32, wherein the computer program code is further adapted to:~~rejected messages are URL requests, each URL request having at least one URL component, wherein the computer program code is further adapted to: store rejected URLs in a trie structure, wherein each node in the trie structure is associated with a URL component; maintain a frequency for each node associated with a URL component, wherein the frequency is a function of a number of occurrences with which a URL component and its descendants were rejected with a rule; select a node with the frequency exceeding a threshold; and generate an exception rule for the selected node and its descendants~~

reject a third message based on a second rejection rule, the second rejection rule rejecting messages having a number of cookies different from a previously indicated number of cookies;

increment a second count of the number of messages from the user received via the one or more user sessions within the predetermined amount of time and rejected based on the cookie number attribute;

based on the second count, determine a second frequency with which messages with the cookie number attribute were rejected based on the second rejection rule;

generate an exception rule to the rejection rule in response to determining that the second frequency exceeds a threshold within the predetermined amount of time;

receive a third message having the cookie number attribute; and

allow the fourth message, responsive to the second exception rule.

.

42. (Currently Amended) The computer program product of claim ~~32~~41, wherein the third message is a message responsive to an earlier message ~~computer program code is further adapted to generate the exception rule by inferencing a scalar data type of the descendants of the selected node~~.

43. (Currently Amended) The computer program product of claim ~~32~~41, wherein the third message is a message responsive to an earlier message, the earlier message providing the previously indicated number of cookies ~~function is an aggregate of a number of occurrences with which the URL component was rejected by a rule and a number of occurrences with which descendants of the URL component were rejected with the rule~~.

44. (Original) The computer program product of claim 32, wherein the computer program code is further adapted to determine the threshold as a product of a total number of messages over a time interval and a percentage of the messages that should be allowed to pass.

45-46 (Cancelled).

47. (Currently Amended) ~~The computer-implemented method of claim 1, further comprising~~ A computer-implemented method for adaptively filtering messages routed across a network by generating exception rules to rejection rules based on attributes of messages previously received and rejected, the method comprising:

receiving, by the security gateway, a first message from a user, the first message comprising a webpage that includes a password field and a user login field;

rejecting, by the message filter, the first message based on a ~~second~~ rejection rule for a field attribute, the field attribute indicating that one of the password field or the user login field exceeds a predetermined number of characters;

incrementing, by the learning engine ~~for the attribute~~, a ~~second~~ count of messages from the user received via one or more of a plurality of user sessions ~~and~~ within a predetermined amount of time and rejected based on the field attribute;

determining, by the learning engine based on the ~~second~~ count ~~for the field attribute~~, a ~~second~~ frequency with which messages having the field attribute were rejected based on the ~~second~~ rejection rule;

generating, by the learning engine, an ~~second~~ exception rule to the ~~second~~ rejection rule in response to the determined ~~second~~ frequency exceeding ~~the predetermined~~ a threshold within the predetermined amount of time;

receiving, by the security gateway, a second message having the field attribute; and

allowing, by the adaptive filter, the second message responsive to the ~~second~~ exception rule.

48. (New) The method of claim 47, wherein the frequency is a weighted count of occurrences of the field attribute.

49. (New) The method of claim 47, wherein the frequency is a direct count of occurrences of the field attribute.

50. (New) The method of claim 47, wherein the threshold is a product of a total number of messages over a time interval and a percentage of the messages that should be allowed to pass.

51. (New) A system for adaptively filtering messages routed across a network by generating exception rules to rejection rules based on attributes of messages previously received and rejected, the system comprising:

a receiver which receives a first message from a user, the first message comprising a webpage that includes a password field and a user login field;

a filter which rejects the first message based on a rejection rule for a field attribute, the field attribute indicating that one of the password field or the user login field exceeds a predetermined number of characters;

a learning engine, for incrementing, a count of messages from the user received via one or more of a plurality of user sessions within a predetermined amount of time and rejected based on the field attribute, for determining, based on the count, a frequency with which messages having the field attribute were rejected based on the rejection rule, and for generating an

exception rule to the rejection rule in response to the determined frequency exceeding a threshold within the predetermined amount of time; and wherein

the filter applies the exception rule to subsequent messages to determine whether to allow the subsequent messages.

52. (New) The system of claim 51, wherein the frequency is a weighted count of occurrences of the field attribute.

53. (New) The system of claim 51, wherein the frequency is a direct count of occurrences of the field attribute.

54. (New) The system of claim 51, wherein the threshold is a product of a total number of messages over a time interval and a percentage of the messages that should be allowed to pass.

55. (New) A computer program product comprising: a computer-readable medium having computer program code embodied therein for adaptively filtering messages routed across a network by generating exception rules to rejection rules based on attributes of messages previously received and rejected, the computer program code adapted to:

receive a first message from a user, the first message comprising a webpage that includes a password field and a user login field;

reject the first message based on a rejection rule for a field attribute, the field attribute indicating that one of the password field or the user login field exceeds a predetermined number of characters;

increment, for the attribute, a count of messages from the user received via one or more of a plurality of user sessions within a predetermined amount of time and rejected based on the field attribute;

based on the count, determining a frequency with which messages having the field attribute were rejected based on the rejection rule; and

generate an exception rule to the rejection rule in response to the determined frequency exceeding a threshold within the predetermined amount of time;

receiving a second message having the field attribute; and

allowing the second message based on the exception rule.

56. (New) The computer program product of claim 55, wherein the frequency is a weighted count of the occurrences of the field attribute.

57. (New) The computer program product of claim 55, wherein the frequency is a direct count of the occurrences of the field attribute.

58. (New) The computer program product of claim 55, wherein the computer program code is further adapted to determine the threshold as a product of a total number of messages over a time interval and a percentage of the messages that should be allowed to pass.